

Agpaytech's Research  
3<sup>rd</sup> June, 2024

# Africa's Financial Fortress:

Exploring Cybersecurity Levy for  
Transactional Safety

# Executive Summary

---

In 2023, the losses reported due to financial investment scams became the most of any crime type tracked. Investment fraud losses rose from \$3.31 billion in 2022 to \$4.57 billion in 2023, a 38% increase. Within these numbers, investment fraud with a reference to cryptocurrency rose from \$2.57 billion in 2022 to \$3.96 billion in 2023, an increase of 53% (Federal Bureau of Investigation's Internet Crime Report, 2023).

Most of such crimes targeted financial transactions and institutions in Africa. With the rapid digitization of financial services across the continent, cybercriminals are exploiting vulnerabilities to perpetrate fraudulent activities. Protecting against the threats of financial fraud poses an increasing concern for businesses, regulatory authorities and consumers in the ever-growing digital payment landscape.



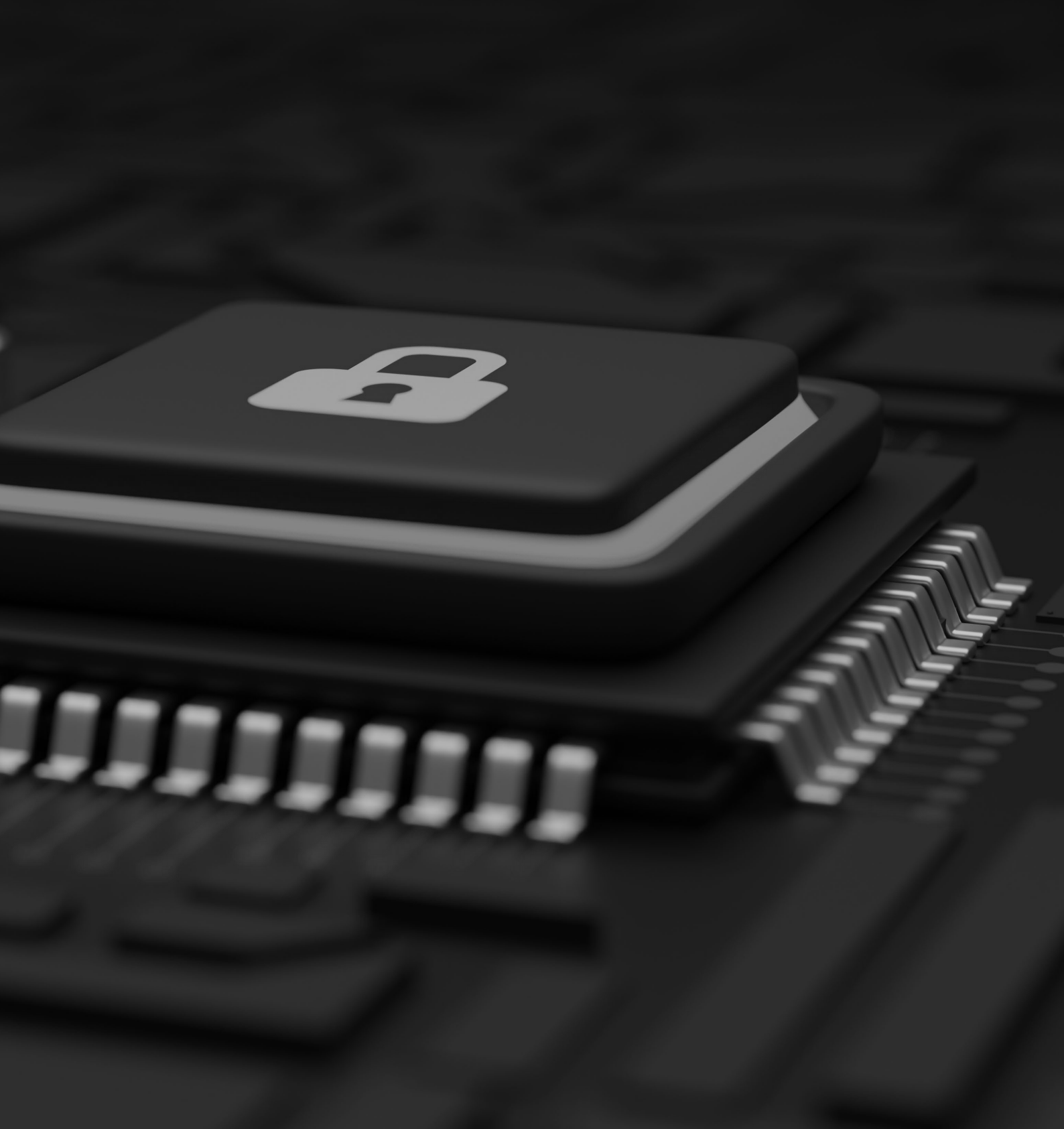
**Investment fraud losses rose from \$3.31 billion in 2022 to \$4.57 billion in 2023, a 38% increase.**

## **How do financial institutions strengthen cybersecurity on financial transactions and data?**

For some organizations, it has become costive and complex to safeguard their organizations' and consumers' data from cyber-attacks, especially considering the availability of sophisticated technologies used by such attackers to perpetrate fraudulent financial activities. Already, there are several cybersecurity defense systems that financial institutions have implemented. Yet, many financial institutions are overburdened by the cost of sustaining cybersecurity technologies. How do FIs fund cybersecurity technologies and campaigns? This report explores the strategies for combating financial cybercrimes and proposes the implementation of a cybersecurity levy on consumers' originating transactions to bolster defenses and reduce the one-way cost of business.

# Table of Content

Executive Summary	-----	2
Global Financial Cybercrime Threats	-----	5
Africa: Cybercrime Cases in the Financial Sector	-----	8
Types of Financial Cybercrime Activities	-----	10
Who Are Behind Financial Cybercrimes?	-----	11
Cyber-fraud transformation and security changes	-----	12
Ways of Combating Financial Transaction Cybercrime	-----	14
Introducing Cybersecurity Levy on Financial Transactions	-----	15
How Cybersecurity Levy Impacts Financial Technology	-----	17
Conclusion	-----	18
References	-----	18
About Agpaytech	-----	19

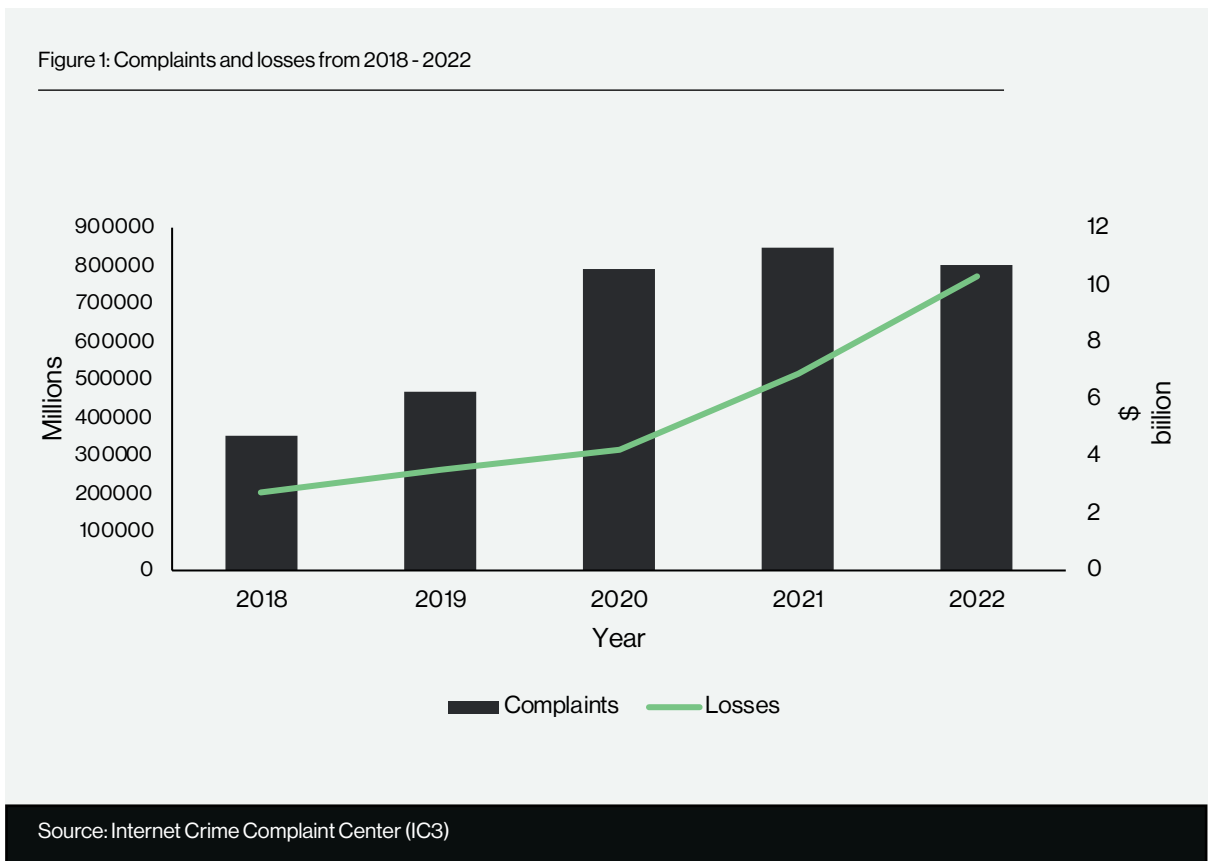


# Global Financial Cybercrime Threats

# Global Financial Cybercrime Threats

The modern digital environment faces countless threats from various malicious entities and individuals equipped with the means to execute extensive fraud operations, extort money and sensitive information, and pose risks to financial security. Whether motivated by financial gain or political agenda, cyber criminals and state-sponsored actors possess the capacity to cripple entire financial institutions and businesses. For example, the Federal Bureau of Investigation's Internet Crime Report (2023) recorded an average of 758,000 cybercrime complaints per year. These complaints address a wide array of Internet scams affecting individuals across the globe. FBI's IC3 from 2019 to 2023 received a total of 3.79 million complaints, reporting a loss of \$37.4 billion.

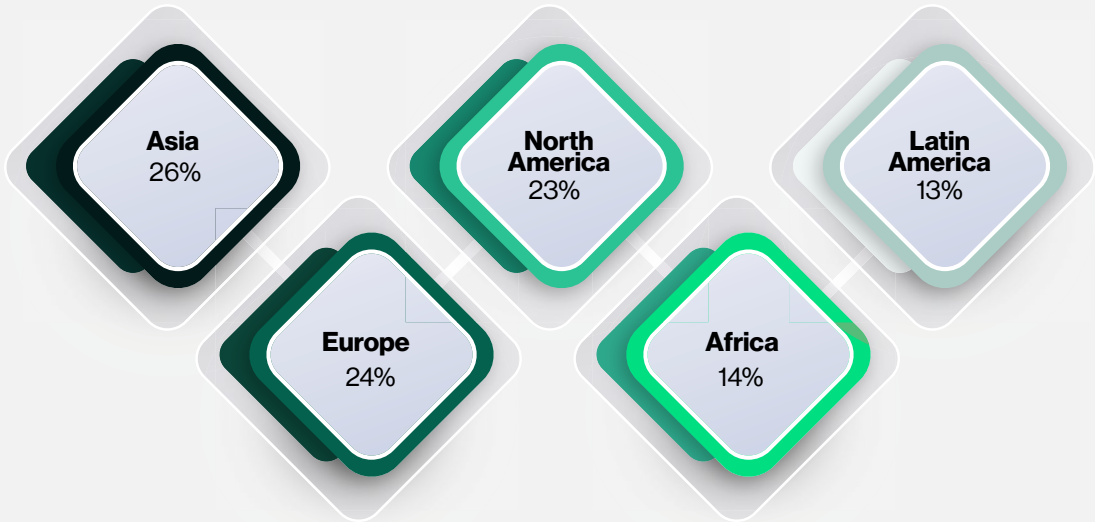
Figure 1: Complaints and losses from 2018 - 2022



The African continent is experiencing remarkable progress and advancement in the realm of digital technology, especially in financial technology (FinTech), digital payments, smart cities and online commerce. Nonetheless, this swift transition to digital platforms has introduced a spectrum of security risks with significant consequences. Exploiting the growing dependence on technology, malicious actors employ diverse tactics to pilfer personal information and perpetrate deceitful actions. Noteworthy cyber threats prevalent in the region encompass digital blackmail, ransomware attacks, intricate online frauds such as phishing, and schemes like business email compromise (BEC).

Protecting against the threats of financial fraud poses an increasing concern for businesses, regulatory authorities and consumers in the ever-growing digital payment landscape. For some organizations, it has become costly and complex to safeguard their organizations and consumers from cyber-attacks, especially considering the availability of sophisticated technologies used by such attackers to perpetrate fraudulent financial activities. For instance, the average cost of a data breach worldwide was recorded at \$4.35 million. Also, 46% of organizations pay ransom after a ransomware attack. According to AAG (2022), 2021 saw an average of \$787,671 lost every hour due to data breaches. 39% of UK businesses reported suffering a cyber-attack in 2022. Moreover, between January to June 2023, Ghana recorded 49.5m direct financial losses through financial fraud activities, this excludes unreported cases. In 2021, Asian organizations suffered the most attacks worldwide. The percentage of attacks against organizations by continent in 2021, (26%), Europe (24%), North America (23%), and others.

Figure 2: Where are organizations most at risk of cybercrime?



Source: AAG





## INNOVATION

1011001110101010001010101010101100110011101010  
0100011101010100010101010101011001100111010101  
101010111011000

[ DATA ] ———— □

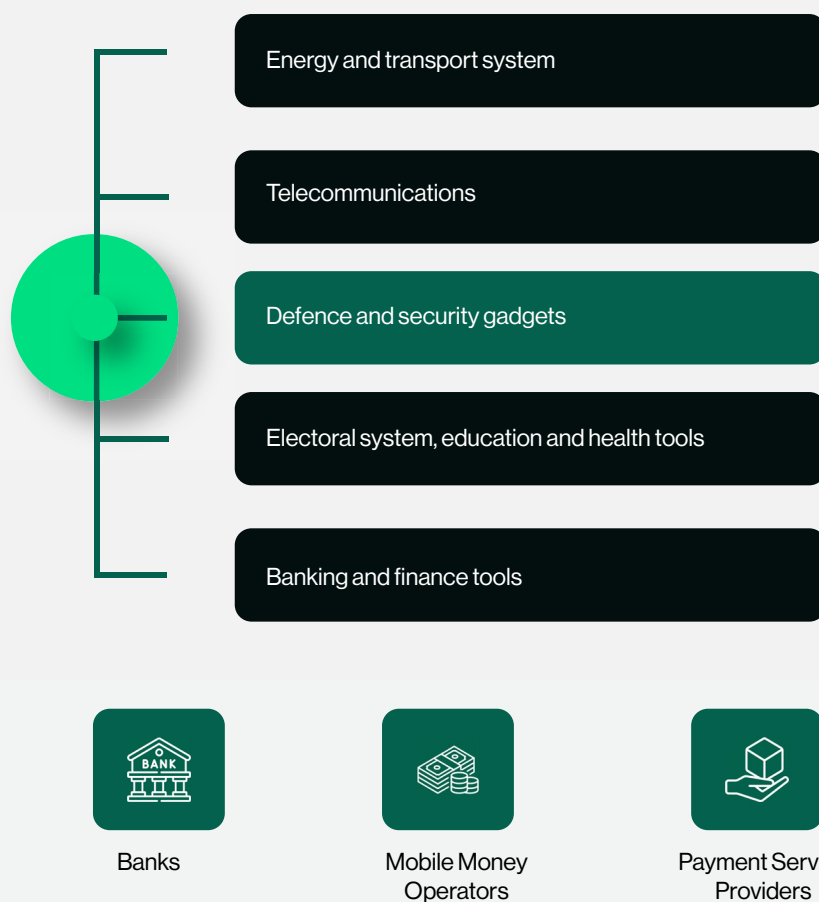


# Africa: Cybercrime Cases in the Financial Sector

# Africa: Cybercrime Cases in the Financial Sector

Cybercrime activities affect several critical information infrastructures such as banking and finance tools, telecommunications, defense and security gadgets, electoral, education and health machines, and energy and transport systems. Yet, the number of cases and implications on the financial sector is a threat to livelihood and industrialization. Since perpetrators demand financial benefits, they usually target banking and financial institutions more than other sectors.

Figure 3: Critical information infrastructure



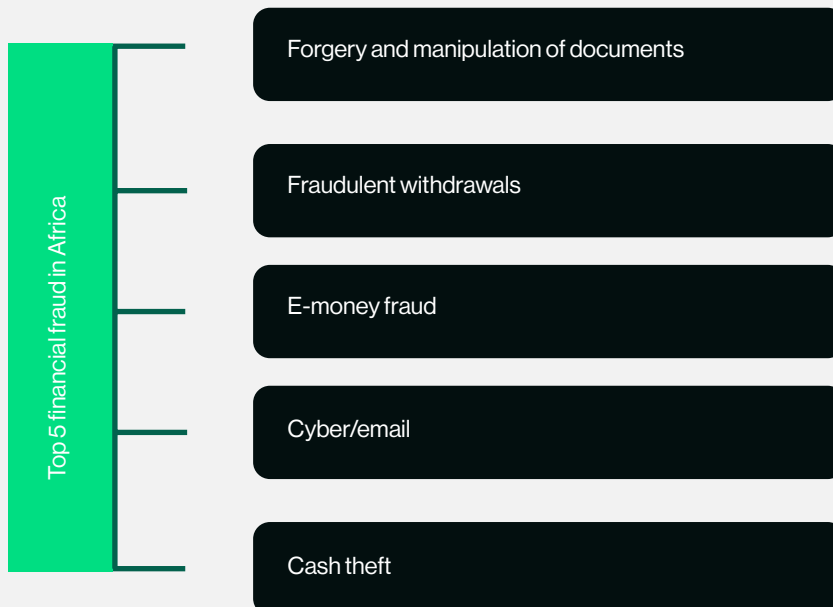
Source: Agpaytech

There are thousands of financial crimes recorded in Africa. In some, there are cases of malicious insiders exploiting their privileged access and technology knowledge to perpetrate theft against their employers.



- For example, the theft of \$3.2 million from a South African bank forced the bank to spend over \$58 million on investigation and mitigation efforts (Cimpanu, 2020).
- In May 2016, an OCG targeted South Africa's Standard Bank, compromised internal banking systems, customer databases, and operational safeguards, and managed to use forged cards to withdraw over \$19 million from ATMs across Japan (Carnegie Endowment for International Peace 2021).
- In January 2018, an OCG stole at least KSh 29 million (approximately \$261,000) from the National Bank of Kenya, and anecdotal reporting suggested the actual sum was about Ksh 340 million (approximately \$3 million) (PC Tech Magazine 2018). The bank cited a compromise of its internal network.
- The Bank of Ghana recorded 2,998 fraud cases amounting to GH¢56 million in 2022 (BoG's Banks and SDI Fraud Report, 2020). In 2020, the Central Bank of Ghana observed a 584.1 percent year-over-year surge in card fraud incidents impacting customers in Ghana (Ghanaian Times 2020).
- In a 2024 debit card fraud incident, hackers targeted Kenya-based Equity Bank, making away with \$2.1 million. The perpetrators reportedly executed a "card-not-present" scam, using stolen card details to shop online, to defraud unsuspecting victims. Typically, the funds are finally moved to other bank accounts. It was discovered that KSh 179.6 million (\$1.3 million) was paid out fraudulently to the 551 Equity Bank accounts between April 9 and 15, 2024. Safaricom received KSh 63 million (\$478,360), with KSh 39 million (\$296,015) going to eleven commercial banks.

Figure 4: Top 5 financial cybercrimes in Africa



Source: Bank of Ghana Fraud Report 2022

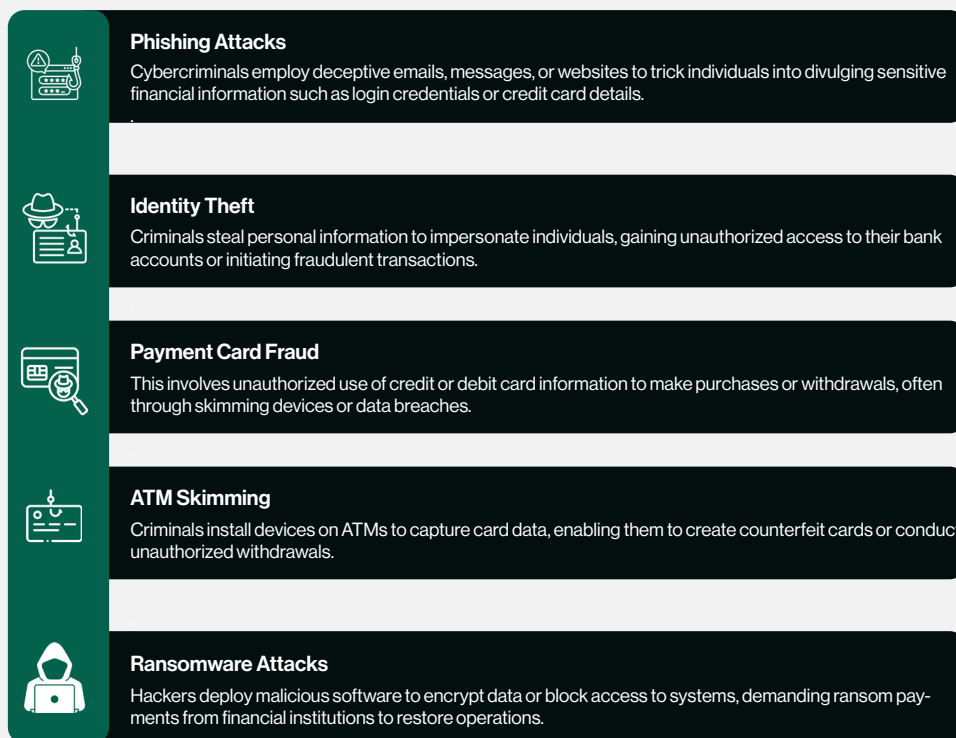
# Types of Financial Cybercrime Activities

Financial institutions in Africa are presently confronted with a substantial danger posed by organized criminal groups (OCGs) and financially incentivized individuals engaging in payment-process theft schemes. Financial fraud and theft cases in Africa encompass various forms of illicit activities that impact economic progress and development. These include mobile money fraud, cyber fraud, financial crimes like embezzlement, theft, bribes, money laundering, illicit financial flows, and economic and financial delinquency involving illegal activities for monetary gain.

These fraudulent practices involve sophisticated methods such as deception, exploitation of

confidential information, and seeking illicit gains through criminal activities. These operations follow successful endeavors seen in more digitally mature developed regions, targeting vulnerabilities in cybersecurity measures to tamper with payment processing mechanisms and internal security protocols. The majority of the fraud typologies are observed in relation to services by Banks, Specialized Deposit-Taking Institutions (SDIs) and Payment Service Providers (PSPs). Cybercrime in the financial sector of Africa encompasses various illicit activities, including but not limited to identity theft, payment card fraud, ATM skimming, ransomware attacks, phishing attacks and forgery activities.

Figure 5: Major financial cybercrimes process



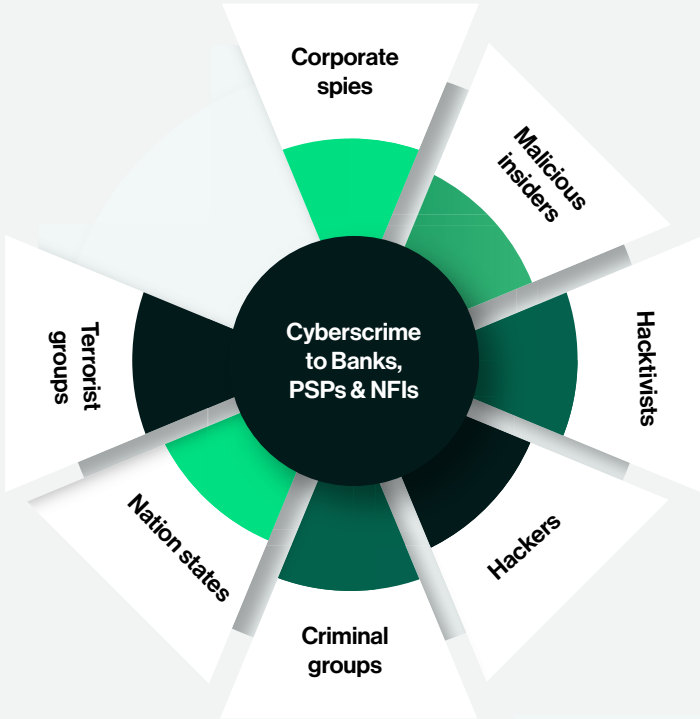
Source: Agpaytech

# Who Are Behind Financial Cybercrimes?

Financial cybercrimes in Africa, like elsewhere in the world, can be perpetrated by a variety of actors, ranging from individual hackers to organized criminal groups and even state-sponsored entities. Individual hackers may target individuals, businesses, or financial institutions for financial gain or simply to demonstrate their technical prowess. Organized criminal groups often operate across borders and may have sophisticated capabilities for carrying out large-scale cybercrimes. These groups may engage in activities such as hacking into banking systems, stealing financial information, or conducting ransomware attacks to extort money from victims.

Additionally, there have been instances where state-sponsored actors from various countries have been implicated in cybercrimes targeting financial institutions or infrastructure in Africa. These actors may have geopolitical motivations or seek to destabilize economies for strategic purposes.

Figure 6: Cybercrime organizers



Source: Agpaytech

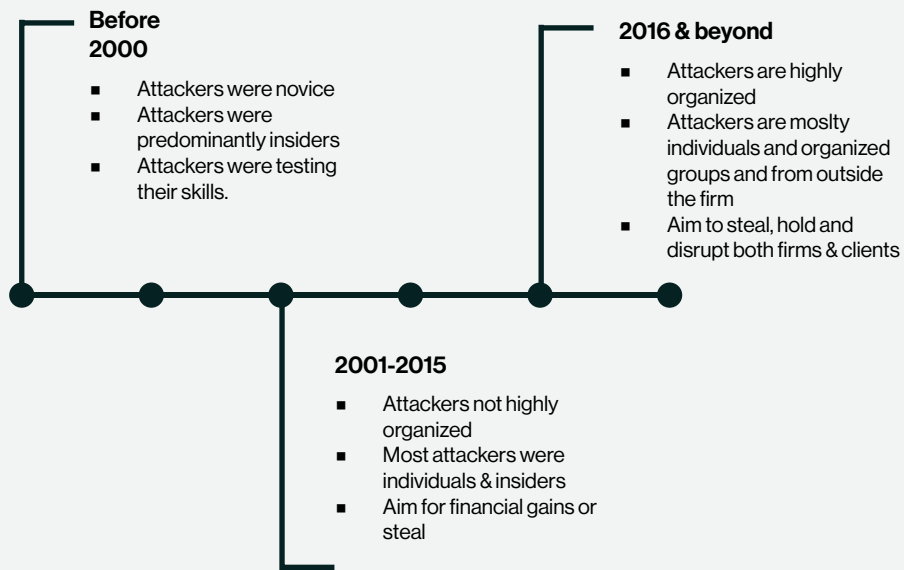
A grayscale background image of a hand with a glowing white fingerprint icon overlaid on the index finger. The icon consists of concentric circles and a central fingerprint pattern. The overall image is semi-transparent, allowing the background to be visible.

# Cyber-fraud transformation and security changes

In recent years, Africa has witnessed a surge in cybercrime targeting financial transactions. With the rapid digitization of financial services across the continent, cybercriminals are exploiting vulnerabilities to perpetrate fraudulent activities. Businesses that neglect to guarantee their staff receive comprehensive training to identify and respond to these threats by employing appropriate security measures, technologies, and detection systems, consequently, not only encounter a heightened possibility of monetary loss, encompassing asset depletion, but also an increased likelihood of harm to their reputation and operational disruptions.







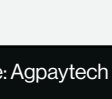
More importantly, the methods of attack are constantly changing and adjusting to bypass the defenses set up by organizations. Predictably, there's been an increase in the utilization of technology by criminals. These attack methods typically exploit vulnerabilities in technology as well as human behavior, sometimes exploiting both simultaneously. This underscores the critical need to regularly assess internal procedures and protocols, ensuring that all staff members are adequately trained and understand their roles in case of a potential attack.

Figure 7: Changing trends of cybercrimes



Source: Agpaytech

Figure 8: Cybercrime changes over time

	Type	Past	Present
		Before 2010	After 2010
	ICT knowledge	Low ICT knowledge	High ICT knowledge
	Digitalization	Low digitization	High digital adoption
	Transfer speed	Non-real time	Real-time
	Threat frequency	One-off operation	Multiple attacks
	Attackers	Individuals	Individuals & organized groups
	Focus	High individuals less organizations	High individuals High organizations
	Victims	Opportunistic	Specifically targeted






Source: Agpaytech



# Ways of Combating Financial Transaction Cybercrime

Several experts, organizations and countries have designed strategies to curb cybercrime activities that target critical information infrastructure at the individual, organization and national levels. For instance, countries like Ghana, Kenya, Uganda, Australia, the European Union (EU), Nigeria, India, USA, China, Singapore, etc., have documented national cybersecurity strategies. Some countries like the USA, Europe, Ghana, and Kenya published annual reports on cybercrimes in the banking and other sectors. The fight against cybercrimes has led central banks and security experts to design strategies and mechanisms for effective cybersecurity for the public and private sectors by combining good governance with a set of technological initiatives and interventions.

Table 1: Fighting against cybercriminals

	Measures	What to do
	Enhanced security protocols	Implementing multi-factor authentication, encryption, and intrusion detection systems to safeguard financial data.
	Cybersecurity awareness training	Educating employees and customers about common cyber threats and best practices for securing personal and financial information.
	Collaborative efforts	Establishing partnerships between financial institutions, law enforcement agencies, and cybersecurity experts to share threat intelligence and coordinate responses to cyber incidents.
	Regulatory compliance	Enforcing stringent regulations and standards for data protection, cybersecurity, and incident reporting within the financial sector.
	Investment in Technology	Deploying advanced cybersecurity solutions such as artificial intelligence, machine learning, and behavioral analytics to detect and prevent cyber threats in real time.

Source: Agpaytech

# Introducing Cybersecurity Levy on Financial Transactions

To finance these cybersecurity initiatives effectively, the introduction of a cybersecurity levy could be considered. This levy would entail a small, mandatory fee imposed on financial transactions, collected by regulatory authorities or financial institutions. The funds generated would be allocated towards strengthening cybersecurity infrastructure, conducting cyber awareness campaigns, and supporting cybercrime investigations and prosecutions. By spreading the financial burden across transactions, the levy ensures sustainable funding for cybersecurity efforts while minimizing individual costs for businesses and consumers. The introduction of a cybersecurity levy needs to be strategic to avoid public or consumers' wrath. The levy process must be open to all stakeholders and opinion leaders to avoid political sentiments.

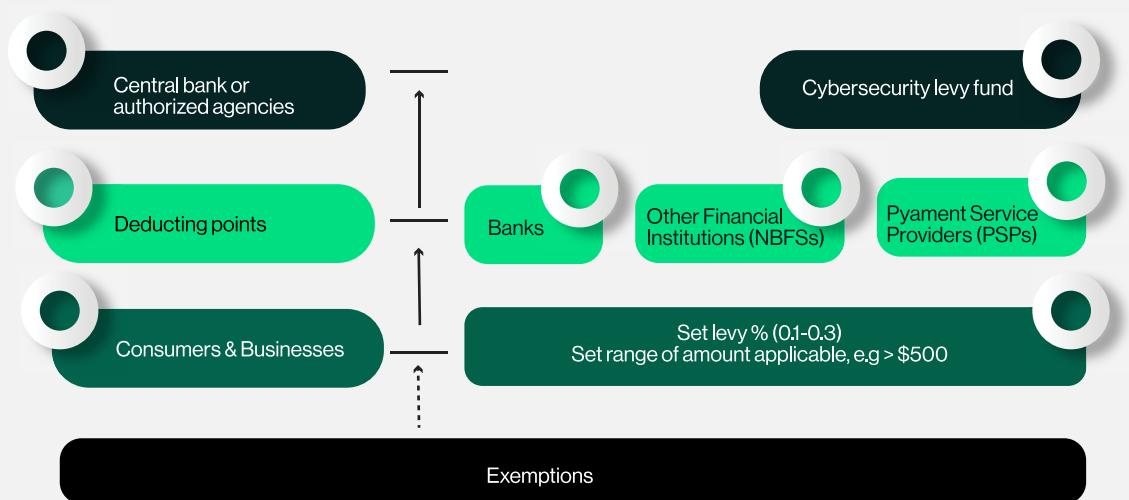
Figure 9: Cybersecurity levy adoption strategy



Source: Agpaytech

Implementing an effective cybersecurity levy in Africa requires careful planning and consideration of various factors. First, it is essential to engage with relevant stakeholders including government agencies, financial institutions, cybersecurity experts, and industry associations to garner support and gather insights into the specific needs and challenges of the African region. Besides, there is the need to develop a regulatory framework outlining the legal basis, scope, and objectives of the cybersecurity levy. This framework should define the types of financial transactions subject to the levy, exemptions, collection mechanisms, and utilization of funds. For effective cybersecurity levy implementation, the authorities in charge should assess the appropriate structure for the levy, considering factors such as transaction volume, value, and frequency. Options may include a fixed fee per transaction, a percentage of transaction value, or a combination of both. Next is to implement robust collection mechanisms to ensure efficient and transparent levy collection. This may involve collaboration with financial institutions, payment processors, and regulatory authorities to integrate levy collection into existing transaction processes. More importantly, justifying the purpose of the levy is essential to its adoption. There should be clear guidelines for the utilization of levy funds, prioritizing investments in cybersecurity infrastructure, training and capacity building, research and development, and cybercrime prevention initiatives.

Figure 10: Cybersecurity levy collection mechanism



Source: Agpaytech

# How Cybersecurity Levy Impacts FinTechs

---

Introducing a cybersecurity levy on consumers' financial transactions could have several impacts on banks and FinTechs in Africa. It largely depends on how it is implemented, the level of collaboration between industry stakeholders and governments, and the effectiveness of measures taken to mitigate potential negative consequences.

Positively, the introduction of a cybersecurity levy could incentivize greater collaboration and information sharing among industry stakeholders, including FinTech firms, financial institutions, regulators, and cybersecurity experts. Pooling resources and expertise could enhance the collective ability to combat cyber threats effectively. It could also serve as an opportunity to raise awareness among consumers about the importance of cybersecurity and the risks associated with financial transactions. Financial education initiatives could help empower consumers to protect themselves against cyber threats.

Negatively, consumers may bear the brunt of the cybersecurity levy through increased transaction fees or charges on their financial transactions. This could potentially make financial services more expensive for end-users, which might discourage adoption, particularly among those who are financially marginalized.

African countries have been making strides in promoting financial inclusion through FinTech solutions. Imposing a cybersecurity levy could hinder these efforts by making financial services less accessible or affordable for underserved populations, thus widening the gap between the banked and unbanked. Also, FinTech startups and struggling financial institutions operating in Africa may face increased costs due to the cybersecurity levy, which could impact their ability to innovate and compete. Additionally, some investors might be deterred by the additional financial burden imposed by the levy, potentially leading to a slowdown in investment in the African FinTech sector.

# Conclusion

---

Cybercrime poses a significant threat to financial transactions in Africa, undermining trust, financial stability, and economic development. However, through proactive measures such as enhanced security protocols, cybersecurity awareness, collaborative efforts, and the introduction of a cybersecurity levy, the continent can strengthen its defenses against cyber threats and safeguard financial systems for the benefit of all stakeholders. It is vital for governments, regulatory bodies, financial institutions, and other stakeholders to prioritize cybersecurity and work together toward building a resilient and secure digital financial ecosystem in Africa. A cybersecurity levy on financial transactions may provide additional funding for cybersecurity initiatives, but the levy should be applicable to a range of amounts and a specified amount such as 0.2% on consumers originating transactions greater than \$500.

# References

---

- Dartnall, Robert; Palmer, Kit; Ruttenberg, Wiebe. Cyber Threats to the Financial Sector in Africa: An Assessment of the Current Threat and an Analysis of Emerging Trends on the Future Threat Landscape (English). Washington, D.C.: World Bank
- Group. <http://documents.worldbank.org/curated/en/099830405172214598/P16477000601530760af01093740e385fe8>
- <https://aag-it.com/the-latest-cyber-crime-statistics/>
- <https://www.citigroup.com/global/insights/commercial-bank/an-overview-of-fraud-and-cybersecurity->
- Internet Crime Complaint Center (IC3)
- Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527



# About Agpaytech Ltd.

Agpaytech Ltd. is a company pioneering in the Fintech space with a focused approach to building robust technologies for e-commerce Card Processing Solutions for Payment Service Providers (PSPs). Additionally, we provide Compliance and Regulatory Umbrella, Remittance-as-a-Service (RaaS), Banking-as-a-Service (BaaS), Foreign Exchange, Cross Border Payments, and digital currency technology.

We also provide practical white paper research support to central banks, government and private institutions, economic organizations, and NGOs in Africa. Our services expand from research projects, state-of-industry reports, project assessment, data collection, and consulting services in the fintech space.

## Contact Us

### United Kingdom

AGPAYTECH LTD.  
3rd Floor, 86-90 Paul Street  
London, EC2A 4NE,  
United Kingdom

### United States of America

AGPAYTECH USA LLC  
9701 Apollo Dr Suite 100  
Largo MD, 20774,  
United State of America

 [www.agpaytech.co.uk](http://www.agpaytech.co.uk)

 [info@agpaytech.co.uk](mailto:info@agpaytech.co.uk)

All rights reserved.

---

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system, without prior permission in writing from Agpaytech Ltd. The mention of specific companies, manufacturers or software does not imply that they are endorsed or recommended by the authors in preference to others of a similar nature that are not mentioned.

© Agpaytech Ltd. 2024.